Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network, wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter;

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;

(d) determining, based on the received first data, whether to query for additional data;

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and

(f) analyzing the security event using at least one of the first data and the additional data.

2. (Original) The method of claim 1 wherein step (a) further comprises determining at least one of intrusion of the customer network, a port scan, service probes, a signature from an attack, a buffer overflow attempt, a format string attack, a denial of service attempt, a web-based attack, and an attempted rights escalation.

3. (Original) The method of claim 1 wherein step (a) further comprises monitoring the customer network for the security event.

4. (Original) The method of claim 1 wherein step (a) further comprises determining at least one of nature of the security event, likelihood that the security event is harmful, and impact of the security event.

5. (Original) The method of claim 1 wherein step (a) further comprises detecting, by the data monitor, the occurrence of the security event.

6. (Original) The method of claim 1 wherein the security event further comprises a potential security event.

7. (Original) The method of claim 1 wherein at least one of the first component and the another component of the customer network further comprises at least one of the data monitor and a client computer.

8. (Original) The method of claim 1 wherein step (b) further comprises querying, by the data monitor, the component.

9. (Original) The method of claim 1 wherein step (c) further comprises at least one of

(i) transmitting the received first data to a security analysis module for analysis, and

(ii) analyzing the first data.

10. (Currently Amended) The method of claim 1 wherein step (d) further comprises analyzing the first data to determine whether to query ~~to~~ for additional data.

11. (Original) The method of claim 1 wherein step (d) further comprises determining, by the data monitor, whether to query to additional data.

12. (Original) The method of claim 1 wherein step (f) further comprises populating a trouble ticket during the analysis.

13. (Original) The method of claim 1 wherein step (f) further comprises analyzing, by the data monitor, the security event.

14. (Original) The method of claim 1 further comprising reporting a result of the analysis.

15. (Currently Amended) A method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network, wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter;

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;

(d) determining, based on the received first data, whether to query to additional data;

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and

(f) analyzing, by the data monitor, the security event using at least one of the first data and the additional data.

16-33. (Canceled)

34. (New) The method of claim 1 wherein analyzing the security event is performed by a security analysis module that is not part of the customer network.

35. (New) The method of claim 1 wherein the parameter conveys what type of security event is detected.

36. (New) The method of claim 1 wherein the parameter includes an amount of time elapsed since an occurrence of a previous security event.

37. (New) The method of claim 1 wherein the parameter includes a communication protocol associated with the security event..

38. (New) The method of claim 1 wherein the parameter includes a duration of time of the security event.

39. (New) The method of claim 1 wherein the parameter includes a number of previous occurrences of the security event.

40. (New) A method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network;

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;

(d) determining, based on the received first data, whether to query for additional data;

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and

(f) analyzing the security event using at least one of the first data and the additional data, wherein analyzing the security event is performed by a security analysis module that is not part of the customer network.

41. (New) The method of claim 40 wherein step (a) further comprises determining at least one of intrusion of the customer network, a port scan, service probes, a signature from an attack, a buffer overflow attempt, a format string attack, a denial of service attempt, a web-based attack, and an attempted rights escalation.

42. (New) The method of claim 40, further comprising determining, by the security analysis module, an impact of the security event if left unresolved

43. (New) The method of claim 40 wherein step (a) further comprises determining at least one of nature of the security event, likelihood that the security event is harmful, and impact of the security event.

44. (New) The method of claim 40 wherein step (a) further comprises detecting, by the data monitor, the occurrence of the security event.

45. (New) The method of claim 40 wherein the security event further comprises a potential security event.

46. (New) The method of claim 40 wherein steps (a), (b) and (e) are performed by the security analysis module.

47. (New) The method of claim 40 wherein step (b) further comprises querying, by the data monitor, the component.

48. (New) The method of claim 40 wherein step (c) further comprises at least one of

(i) transmitting the received first data to the security analysis module for analysis, and

(ii) analyzing the first data.

49. (New) The method of claim 40 wherein step (d) further comprises analyzing the first data to determine whether to query for additional data.

50. (New) The method of claim 40 wherein step (d) further comprises determining, by the data monitor, whether to query to additional data.

51. (New) The method of claim 40 further comprising reporting a result of the analysis.